IP et le Routage

Introduction

Les réseaux informatiques ont ceci d'intéressant: Ils couvrent des besoins aussi simples que la connexion entre deux hôtes sur un réseau local que l'interconnexion de systèmes à l'échelle planétaire.

Ici, nous allons nous intéresser à quelques aspects nécessaires à une bonne compréhension de ce qu'il se passe sur notre connexion Internet par le câble (nous verrons pourquoi cette connexion diffère fondamentalement d'autres moyens comme l'ADSL, le RTC ou l' ISDN).

Vous trouverez dans cet exposé :

- Une définition de ce que sont les adresses MAC et IP.
- Ce que sont les réseaux physiques et les réseaux logiques.
- Quels sont les composants d'interconnexion de réseaux les plus courants.
- Comment les données circulent d'un réseau à l'autre.
- Une manipulation destinée à toucher du doigt les problèmes du routage.

Plan du chapitre

Physique/Logique

Qu'est-ce qu'une adresse MAC ?

Media Access Control

C'est une adresse écrite en "dur" dans le "firmware" d'un équipement réseau, le plus souvent une interface réseau.

Cette adresse est définie sur 6 octets.

- Les trois premiers (les plus à gauche) sont attribués au constructeur.
- Les trois derniers sont spécifiques à un équipement matériel donné.

Au total, une adresse MAC est sensée être unique au monde.

Son but est d'identifier sans aucune ambiguïté possible un nœud sur un réseau. Elle est utilisée par le niveau 2 du modèle OSI pour l'acheminement des données d'une source vers une cible.

Il faut bien comprendre que cette adresse est indispensable, parce qu'elle est la seule qui soit définie à la mise en route d'un système, puisqu'elle réside dans une ROM. D'ailleurs, certains protocoles réseaux simples se contentent de cette adresse pour fonctionner. NetBEUI en est un exemple. De plus, au niveau 2 du modèle OSI, c'est la seule adresse en mesure d'être utilisée.

Toute autre adresse qui sera ajoutée avec l'installation du système sera une adresse plus évoluée, destinée à gérer les réseaux de façon logique, mais l'adresse MAC demeure indispensable.

Avantages et inconvénients

Nous l'avons vu, le principal avantage est que cette adresse unique est disponible immédiatement lors de la procédure de "boot" et qu'elle est alors la seule disponible, de plus, c'est la seule qui soit utilisable dans les couches basses du réseau.

Son principal inconvénient est qu'elle est physiquement attachée à un hôte. Pour en changer, il faut changer d'interface (il y a des astuces pour qu'il en soit autrement, surtout avec Linux, mais je ne vous les dévoilerai pas... Un internaute politiquement correct n'a pas besoin de les connaître). De plus, la répartition de ces adresses sur un réseau est faite de manière quasi aléatoire, il n'y a que le constructeur de l'interface qui maîtrise cette adresse. Il est donc impossible d'organiser cet adressage de manière logique.

Adresse IP

Nous n'allons pas revenir sur les détails de cette adresse, abondamment traités dans le chapitre précédent[1]. Cette adresse sera ici d'une importance fondamentale.

Mise en garde

1 TCP/IP : http://christian.caleca.free.fr/tcpip/index.html

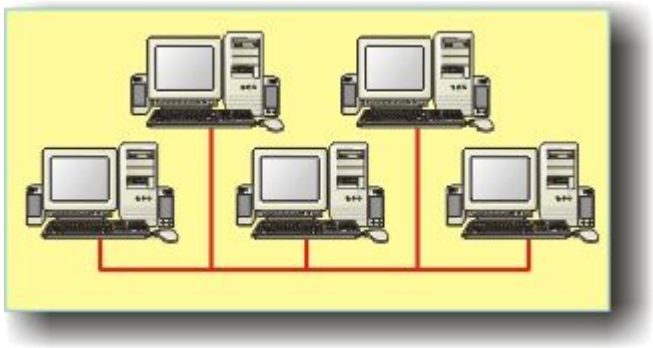
Nous avons dit et redit que la couche 2 n'utilise que l' adresse MAC pour acheminer les données. Au passage de la couche 3 (qui utilise une adresse logique, IP dans notre cas) à la couche 2 (et réciproquement), il faudra donc disposer d'une table d'équivalence entre les adresses IP et les adresses MAC du réseau.

Réseau physique ou logique

Ici, nous allons faire abstraction du support choisi (autant que possible) et nous intéresser à la façon de connecter les systèmes entre eux.

Un réseau physique

Le principe



Voici un réseau physique :

- Tous les hôtes sont connectés entre eux au moyen du même support de transport.
- Tous les hôtes sont en mesure de communiquer entre eux directement, sans besoin d'une quelconque passerelle.

Un réseau physique, c'est relativement facile à comprendre. Vous prenez un HUB, vous y connectez autant de postes que vous pouvez avec des câbles de cuivre en paire torsadée et vous avez construit un réseau physique.

Vous vous arrangez pour que tous les postes disposent du même logiciel réseau, par exemple WIndows avec le protocole NetBEUI et le tour est joué. Vous pouvez partager des ressources entre les postes. Finalement, c'est assez simple. Oui mais, c'est parce que vos besoins sont simples. Si vous voulez utiliser TCP/IP, il faudra alors définir des adresses IP pour chacune de vos machines, adresses choisies dans le même réseau logique (voir le chapitre TCP/IP[2]) et votre réseau fonctionnera aussi bien. Pourtant, NetBEUI n'introduit pas d'adresse logique.

Comment ça marche

La question est très compliquée, mais il est encore possible ici de donner une réponse simple et satisfaisante pour l'instant:

Les informations qui transitent sur le réseau sont visibles par tous les hôtes du réseau. Cependant, un système d'adresse unique par hôte (adresse MAC) permet au destinataire de se reconnaître et de récupérer l'information. Disons que dans un groupe de 5 personnes qui vaquent chacunes à leurs occupations, **vous** posez une question à **un** membre du groupe. Tout le groupe **entend** la question, mais **celui** à qui elle est destinée se **reconnaît** et vous répond. Les autres **entendent** aussi la réponse, mais savent qu'ils ne sont pas concernés et ne **l'écoutent** pas. Notez que si vous êtes capable d'analyser parfaitement tous les mécanismes mis en oeuvre dans cet exemple, vous avez

2 TCP/IP : http://christian.caleca.free.fr/tcpip/index.html

déjà pratiquement tout compris sur les principes des réseaux locaux.

Ça peut se compliquer...

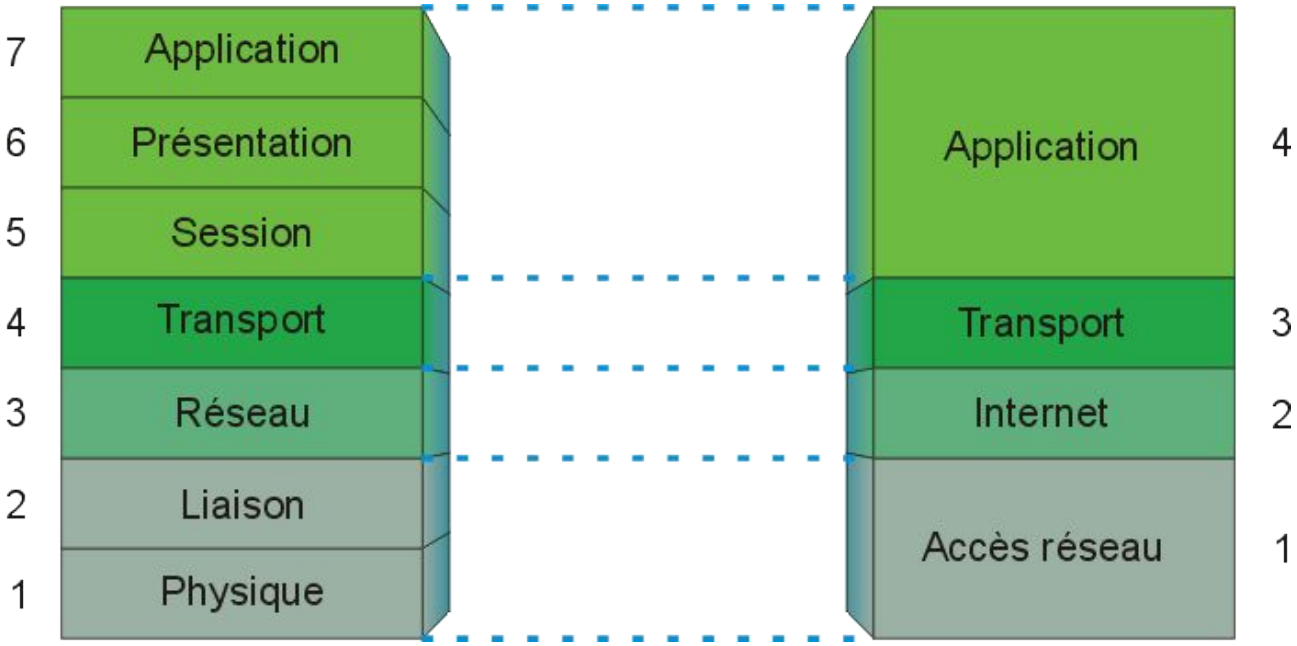
Nous verrons, avec les passerelles, qu'un réseau physique peut être un peu plus compliqué que ça. Les ponts, qui sont des passerelles travaillant au niveau 2 (Avec les adresses MAC) permettent de connecter deux réseaux physiques pour qu'ils n'en fassent plus qu'un.

Un réseau logique

Le principe

La notion de réseau logique est déjà un peu plus délicate, parce qu'elle n'est pas directement liée au câblage.

Il est peut-être nécessaire de reprendre le modèle théorique d'un OS réseau. A gauche, le modèle OSI en 7 couches, à droite le modèle DOD de TCP/IP, plus pragmatique. Nous allons tout de même utiliser le modèle OSI qui décompose mieux les diverses fonctions.



Pour l'étude des réseaux, ce sont surtout les trois premières couches OSI qui nous intéressent. Nous avons déjà parlé de la couche physique et de la couche liaison. Parler d'un réseau physique, c'est parler d'un réseau en le regardant au niveau 2.

Un réseau logique en revanche fait intervenir la couche 3. Il existe toujours une adresse unique par hôte, mais cette adresse est logique, l'adresse IP en ce qui nous concerne, et cette adresse est exploitée par niveau 3.

Comment ça marche

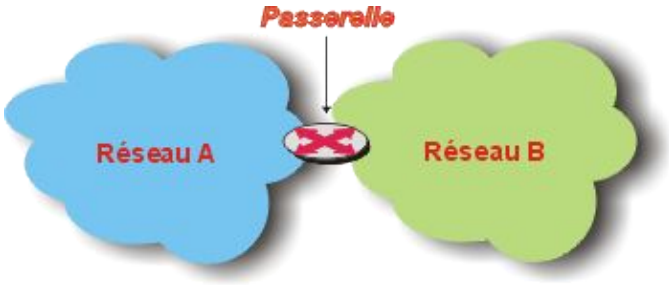
Comme l'adresse utilisée est fixée par une stratégie définie par l'architecte du réseau et non par le hasard de la construction de la machine, il devient possible d'organiser les transferts de données d'une manière optimale en fonction des besoins. Deux réseaux logiques ne pourront communiquer

entre eux que par l'intermédiaire d'un routeur, ce qui permet non seulement d'optimiser les flux de données, mais encore d'assurer un minimum de sécurité parce que l'on va pouvoir effectuer un contrôle d'accès au niveau de ces routeurs (fonctions de "firewalls" ou "parefeu").

Il ne nous reste plus maintenant qu'à regarder d'un peu plus près les passerelles les plus courantes.

Passerelles

C'est quoi, une passerelle ?



Nous allons dire que c'est un élément qui permet d'interconnecter plusieurs réseaux de manière à permettre le passage de l'information d'un réseau à l'autre. Je n'ai volontairement pas précisé s'il s'agissait de réseaux logiques ou physiques, parce que tout est possible dans ce domaine.

Les principales techniques

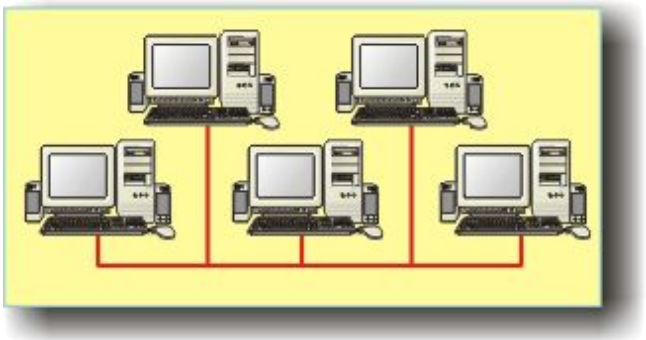
Nous n'allons pas parler de tous les types de passerelles que l'on peut rencontrer, il y en a beaucoup trop. Nous allons regarder d'un peu plus près deux types courants que sont les ponts et les routeurs. Ils ne travaillent pas au même niveau du modèle OSI et ne servent pas tout à fait à la même chose, bien qu'ils soient tous les deux des éléments d'interconnexion.

Comme nous avons vu qu'il existe deux adresses pour un nœud donné: l'une matérielle (adresse MAC) qui est utilisée au niveau 2 et l'autre logicielle (IP le plus souvent) utilisée au niveau 3, nous pouvons nous attendre à trouver des passerelles travaillant aux niveaux 2 : les ponts, ou au niveau 3 : les routeurs.

Les ponts

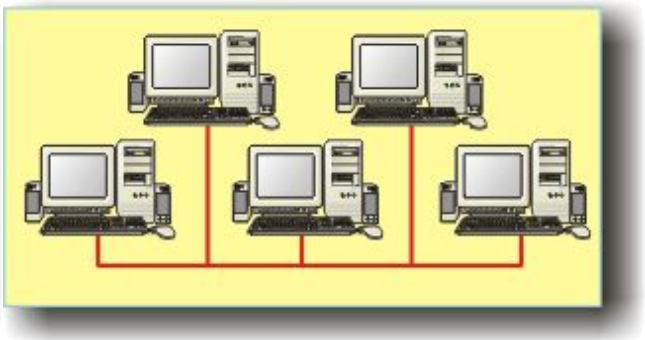
Nous avons deux réseaux physiques Ethernet totalement disjoints. Ces deux réseau utilisent TCP/IP et les hôtes disposent d'adresses IP dans la même classe, avec le même masque de sous réseau. Cependant, il n'existe aucun doublon dans les adresses entre les deux réseaux.

Réseau A



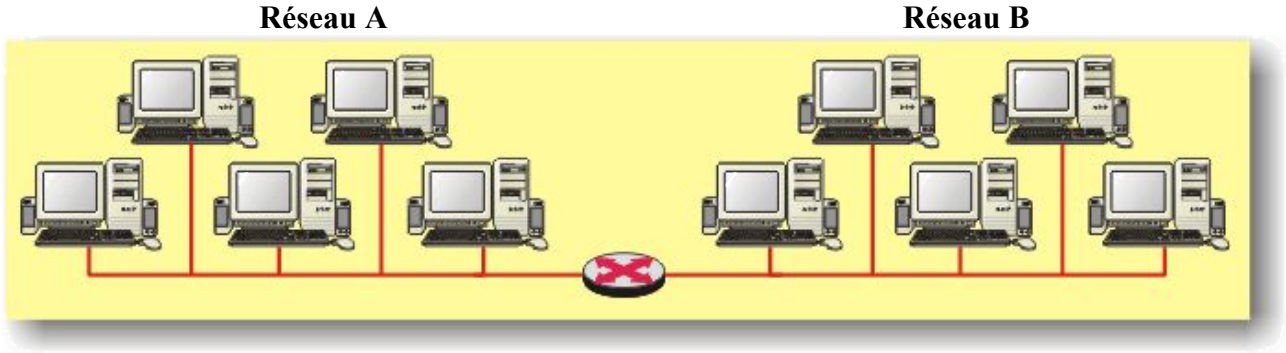
Adresses IP	de 192.168.0.1 à 192.168.0.50
Masque de sous réseau:	255.255.255.0

Réseau B

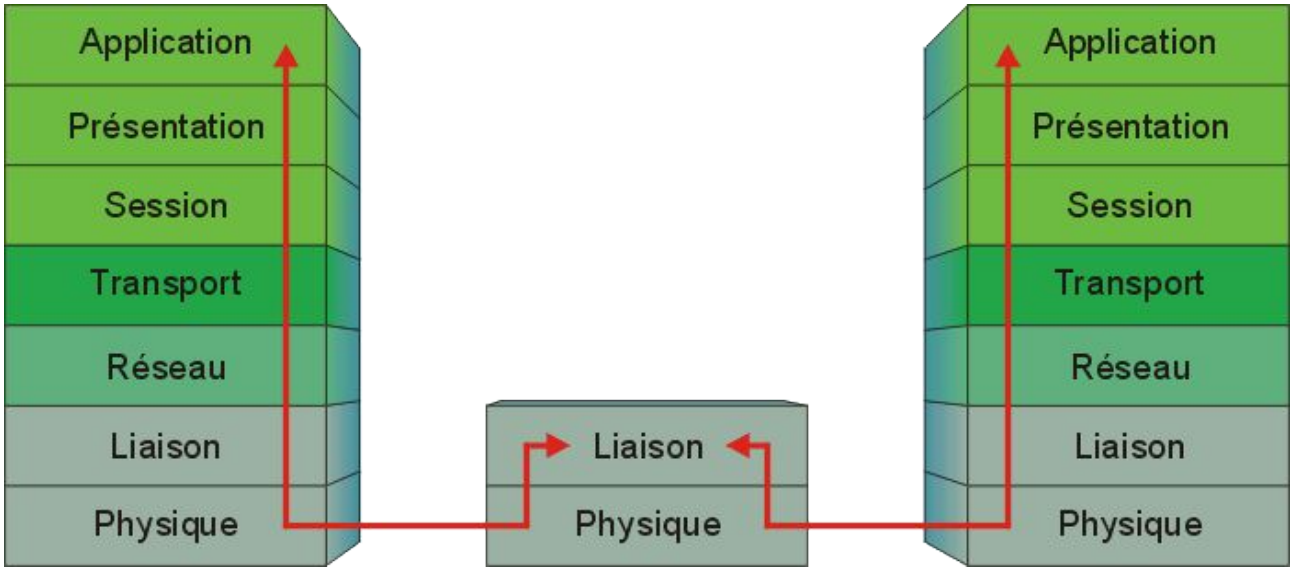


Adresses IP	de 192.168.0.128 à 192.168.0.170
Masque de sous réseau:	255.255.255.0

Nous désirons raccorder ces deux réseaux physiques pour n'en faire plus qu'un et nous allons le faire avec un pont



Qu'est-ce qu'un pont ?



Description générale

Un pont dispose d'un pied dans chaque réseau. Il agit au niveau 2, sur la couche de liaison. Il est capable de laisser passer les trames d'un réseau à l'autre, mais ne le fait pas bêtement.

Un pont, après une période d'apprentissage, sait repérer les adresses MAC des nœuds de chaque côté du pont. Il ne laissera passer d'un côté à l'autre que les trames qui ont réellement besoin de passer; si bien que le trafic sur chaque côté se trouve optimisé, à la condition bien entendu que l'architecture générale ait été pensée dans ce sens. Un pont est très efficace si les deux réseaux A et B communiquent peu entre eux. Si le réseau A utilise principalement les services des serveurs du réseau B et réciproquement, le pont perd complètement son intérêt, autant le remplacer par un bout de câble.

Particularités

- Un pont, travaillant au niveau 2, est indépendant des couches réseau supérieures. En d'autres termes, un pont fonctionnera aussi bien avec TCP/IP qu'avec un protocole non routable (pas

d'adresses logiques) comme NetBEUI.

- Il faut **impérativement** que les protocoles réseau soient les mêmes de chaque côté du pont, l'échange se faisant au niveau des trames.
    - Un pont ne pourra pas interconnecter un réseau Ethernet avec un réseau Token Ring par exemple.
    - Un pont ne pourra pas interconnecter deux réseaux Ethernet, l'un utilisant TCP/IP et l'autre un autre protocole (IPX/SPX par exemple).
- Deux réseaux physiques pontés apparaissent **comme un seul réseau physique**. Au niveau de la couche réseau (et des couches supérieures), le pont est transparent. Ceci est un détail fondamental.

Le principe du pont est repris dans les "switches", que l'on pourrait considérer comme des HUBS évolués.

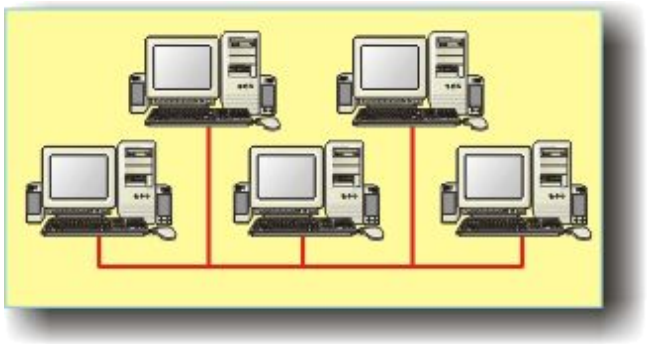
Conclusion

Un pont est une passerelle particulière, que l'on utilise au sein d'un même réseau physique, pour optimiser le trafic des trames sur ce réseau.

Les routeurs

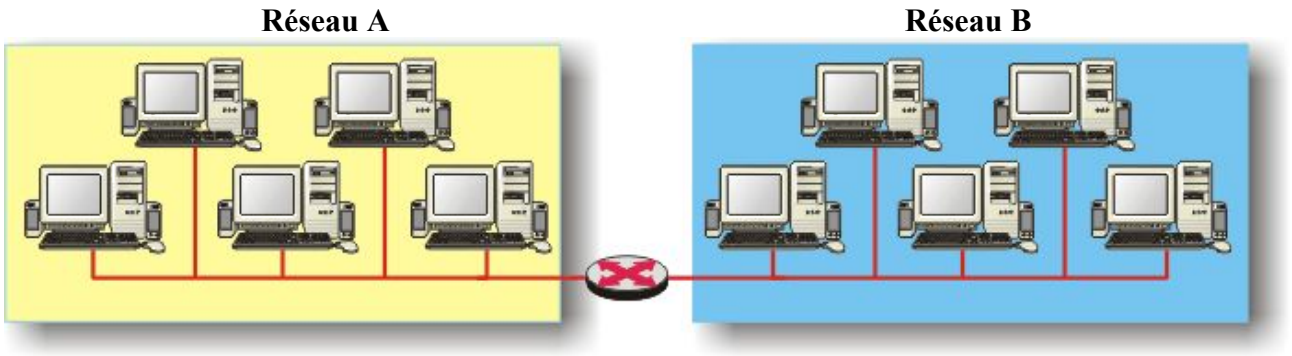
Nous avons ici aussi deux réseaux physiques Ethernet totalement disjoints. Ces deux réseau utilisent TCP/IP mais les hôtes disposent d'adresses IP de réseau différentes (ou de même réseau, mais avec des masques de sous réseaux différents, ce qui introduirait la notion de sous réseau logique.

Réseau A **Réseau B**

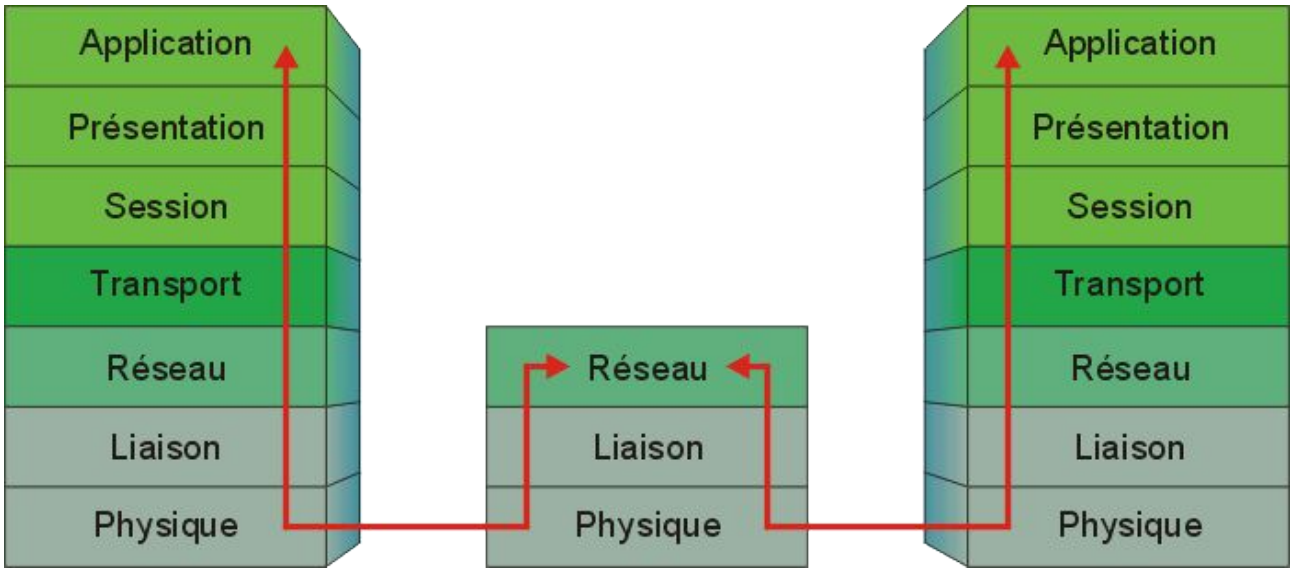


Adresses IP	de **192.168.0**.1 à **192.168.0**.50	Adresses IP	de **192.168.1**.1 à **192.168.1**.50
Masque de sous réseau:	255.255.255.0	Masque de sous réseau:	255.255.255.0

Nous désirons raccorder ces deux réseaux physiques pour qu'ils puissent communiquer, nous allons le faire avec un routeur.



Qu'est-ce qu'un routeur ?



Un routeur agit au niveau de la couche réseau, d'IP par exemple. Le résultat peut paraître similaire à celui d'un pont, il n'en est rien.

Description générale

Le routeur lui aussi dispose d'un pied dans chaque réseau, mais son fonctionnement est plus évolué. Alors que le pont utilise les adresses MAC, le routeur utilise les adresses réseau (IP en ce qui nous concerne).

Particularités

- Les tables de routage ne sont pas construites par un simple apprentissage, comme dans un pont, mais sont mises en place soit à la main, soit automatiquement au moyen de protocoles plus évolués.
- Les deux réseaux raccordés restent deux réseaux physiques différents, les adresses MAC d'un côté restent totalement inconnues de l'autre côté, ce qui n'est pas le cas du pont. (Nous le comprendrons mieux avec les manipulations qui suivent).
- Les réseaux A et B peuvent être de nature différente.

- Le protocole réseau (TCP/IP par exemple) doit tout de même être identique des deux côtés et doit être routable (ce qui n'est pas nécessaire avec un pont).

Notez q'un routeur peut interconnecter plus que deux réseaux, il lui suffit de disposer d'un pied dans chaque réseau à interconnecter. (Des ponts multivoies existent cependant aussi).

D'autres solutions basées sur un principe comparable existent et permettent d'interconnecter des réseaux ayant des protocoles différents, mais ce n'est pas l'objet de cet exposé.

Conclusions

Un routeur permet de faire communiquer deux réseaux logiques différents. Nous verrons plus loin ce que cela induit dans le transport des données. Si l'on interconnecte deux réseaux physiques avec un routeur, il faudra absolument que ces deux réseaux physiques soient également des réseaux (ou sous réseaux) logiques différents (NetID différents). Un routeur conservera la notion de réseaux physiques différents. C'est très important, surtout lorsque l'on utilise des dispositifs comme DHCP pour attribuer des adresses IP aux hôtes du réseau. Un DHCP a une portée limitée à son réseau physique, autrement dit, un DHCP ne peut pas fournir d'adresse à un hôte situé de l'autre côté d'un routeur.

Ah, mais alors, comment se fait-il que chez nous, câblés de Marseille, il n'existe qu'un seul serveur DHCP (62.161.120.11) et qu'il y a pourtant au moins quatre réseaux logiques et qu'en plus, le DHCP n'est dans aucun de ces réseaux?

C'est parce qu'il existe une exception à cette règle, si l'on utilise un agent de relais DHCP. Ce dispositif permet, s'il est installé sur un routeur, de distribuer des adresses IP sur les réseaux interconnectés par ce routeur avec un seul DHCP situé sur l'un de ces réseaux; à la condition bien entendu, que ce DHCP dispose de plages d'adresses correspondant à chacun de ces réseaux, ce qui est le cas pour FTCI. Dans la pratique, l'agent de relais "intercepte" les requêtes des clients DHCP et les retransmet au(x) serveur(s) indiqué(s) dans sa configuration. Vous trouverez plus de détails sur le fonctionnement de DHCP dans le chapitre qui lui est dédié[3] dans ce site

Mais encore...

Il existe bien d'autres dispositifs capables par exemple d'interconnecter des réseaux utilisant des supports différents (optique, cuivre), des protocoles de transport différents (Ethernet, Token Ring) et même des protocoles différents (TCP/IP, IPX/SPX). Nous n'en parlerons pas.

Le masquage d'adresse

En revanche, il existe une technique de passerelle intéressante qui est le masquage d'adresse. Cette technique est bien utile lorsque l'on souhaite interconnecter un réseau privé pour qu'il devienne **client** d'un réseau public. (Client, parce que ça fonctionne bien dans un sens, beaucoup moins bien dans l'autre et nous allons vite comprendre pourquoi).

Ici, le routeur dispose d'une fonction particulière de changement d'adresse logique (IP). Le principe en est détaillé dans le chapitre MASQUERADE[4]. Disons simplement ici que :

- D'un côté, nous avons un réseau privé, avec des adresses IP prises dans un bloc réservé à cet

3 DHCP : http://christian.caleca.free.fr/dhcp/index.html
4 MASQUERADE : http://christian.caleca.free.fr/masquerade/index.html

effet, par exemple 192.168.0.0 Un routeur sur l'Internet qui voit passer une telle adresse doit immédiatement mettre le paquet à la poubelle, ces adresses sont réservées à un usage privé.

- De l'autre côté nous avons une connexion à l'Internet.
- La passerelle entre les deux va disposer :
  - D'une adresse privée du côté du réseau privé (par exemple 192.168.0.250)
  - D'une adresse IP publique, attribuée par le fournisseur d'accès (par exemple 213.56.56.250)

Cette passerelle va permettre à un hôte du réseau privé d'envoyer une requête à un serveur de l'Internet en mettant au passage son adresse publique à la place de l'adresse privée du client. Vu du dehors, on ne verra qu'un seul hôte: la passerelle, c'est la raison pour laquelle ce type d'interconnexion ne permet pas de placer des serveurs publics dans le réseau privé, sauf avec des artifices pas toujours simples, voire impossible à mettre en oeuvre, suivant le produit utilisé. (Linux 2.2.x le permet de façon assez complexe, Linux 2.4.x, avec IPTables, le permet de façon beaucoup plus simple).

Cette solution est celle que j'utilise pour connecter mes 4 hôtes privés à l'Internet et qui va intervenir dans les manipulations que nous ferons plus loin, c'est la raison pour laquelle j'en parle ici.

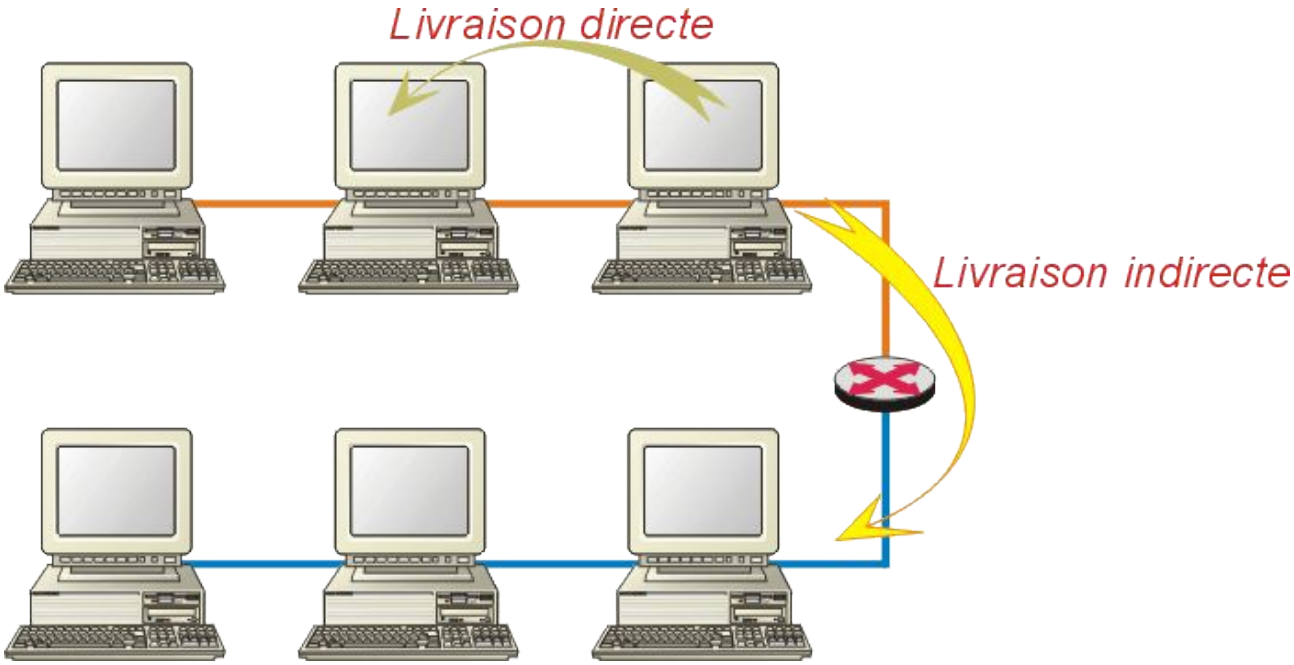
Hormis ce phénomène de changement d'adresse logique, tout va se passer comme avec un "vrai" routeur.

La livraison des données

Voyons un peu les mécanismes mis en oeuvre pour le transport de données d'un hôte à un autre.

Imaginons une application qui doive envoyer des données d'un hôte A1 à un hôte A2. Nous sommes ici sur la couche 7. Les données sont prêtes à être envoyées, elles vont descendre les diverses couches du système. (Nous sommes sur un système TCP/IP)

- D'abord, il faudra résoudre les noms en adresses IP.
- Construire les sockets nécessaires à l'établissement de la connexion.
- Plus bas encore, il va falloir trouver l'adresse physique des hôtes, parce que la couche liaison (couche 2) ne sait utiliser que ce moyen.
  A ce niveau, deux cas de figure peuvent se présenter



La livraison directe

Les deux hôtes sont sur le même réseau physique (et logique), c'est le cas le plus simple. La source et la cible se trouvant sur le même réseau, il suffit qu'il y ait quelque part une table de correspondance entre adresse IP et adresse MAC. Cette table de correspondance est construite localement, sur chaque hôte au moyen du protocole ARP. Cette table ARP est visualisable avec la commande "arp -a"

Exemple :

- Je vérifie que la table ARP est bien vide.
- Depuis mon poste pchris, je fais un ping sur gw1.
- Je regarde à nouveau l'état de ma table ARP.

```
E:\>arp -a
Aucune entrée ARP trouvée

E:\>ping gw1.maison.mrs
```

```
Envoi d'une requête 'ping' sur gw1.maison.mrs [192.168.0.250] avec 32 octets de
données :

Réponse de 192.168.0.250 : octets=32 temps<10 ms TTL=255
Réponse de 192.168.0.250 : octets=32 temps<10 ms TTL=255
Réponse de 192.168.0.250 : octets=32 temps<10 ms TTL=255
Réponse de 192.168.0.250 : octets=32 temps<10 ms TTL=255

Statistiques Ping pour 192.168.0.250:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
minimum = 0ms, maximum = 0ms, moyenne = 0ms

E:\>arp -a

Interface : 192.168.0.10 on Interface 0x1000003
Adresse Internet Adresse physique Type
192.168.0.250 00-20-18-61-90-e3 dynamique
```

Et, bien entendu, mon "sniffeur" embusqué sur gw1 n'a rien perdu de l'échange :

- gw1 est enregistré sous gateway1.maison.mrs (gw1.maison.mrs est un alias)
- pchris est enregistré sous pchris.maison.mrs

```
    No.  Source               Destination          Protocol Info
      1  pchris.maison.mrs     ff:ff:ff:ff:ff:ff     ARP      Who has 192.168.0.250?  Tell
192.168.0.10
      2  gateway1.maison.mrs   pchris.maison.mrs     ARP      192.168.0.250 is at 00:20:18:61:90:e3
      3  pchris.maison.mrs     gateway1.maison.mrs   ICMP     Echo (ping) request
      4  gateway1.maison.mrs   pchris.maison.mrs     ICMP     Echo (ping) reply
      5  pchris.maison.mrs     gateway1.maison.mrs   ICMP     Echo (ping) request
      6  gateway1.maison.mrs   pchris.maison.mrs     ICMP     Echo (ping) reply
      7  pchris.maison.mrs     gateway1.maison.mrs   ICMP     Echo (ping) request
      8  gateway1.maison.mrs   pchris.maison.mrs     ICMP     Echo (ping) reply
      9  pchris.maison.mrs     gateway1.maison.mrs   ICMP     Echo (ping) request
     10  gateway1.maison.mrs   pchris.maison.mrs     ICMP     Echo (ping) reply
     11  gateway1.maison.mrs   pchris.maison.mrs     ARP      Who has 192.168.0.10?  Tell
192.168.0.250
     12  pchris.maison.mrs     gateway1.maison.mrs   ARP      192.168.0.10 is at 00:20:18:b9:49:37
```

Remarquez :

- Ligne 1 la requête ARP émise en broadcast (ff:ff:ff:ff:ff:ff) par mon poste de travail :
  Qui a l'adresse 192.168.0.250 (gw1)? Dites-le à 192.168.0.10 (pchris)
- Ligne 2 la réponse ARP de gw1 à pchris :
  192.168.0.250 est à 00:20:18:61:90:e3

Viennent ensuite les échanges pour la commande ping et enfin (mais ce n'est pas systématique) gw1 qui recherche l'adresse MAC de pchris. Ce n'est pas une bonne idée d'ailleurs, parce qu'il l'a déjà. En effet, si l'on regarde le détail de la trame 1 :

```
Frame 1 (60 on wire, 60 captured)
    Arrival Time: Feb 15, 2001 16:02:12.2750
    Time delta from previous packet: 0.000000 seconds
    Frame Number: 1
    Packet Length: 60 bytes
    Capture Length: 60 bytes
Ethernet II
    Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source: 00:20:18:b9:49:37 (pchris.maison.mrs)
    Type: ARP (0x0806)
    Trailer: 20202020202020202020202020202020...
Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
```

```
    Protocol size: 4
    Opcode: request (0x0001)
    Sender hardware address: 00:20:18:b9:49:37
    Sender protocol address: 192.168.0.10
    Target hardware address: 00:00:00:00:00:00
    Target protocol address: 192.168.0.250
```

On s'aperçoit que l'adresse MAC de pchris est déjà donnée dedans. Et si ça ne suffisait pas, l'information se trouve également dans la trame 2 :

```
Frame 2 (60 on wire, 60 captured)
    Arrival Time: Feb 15, 2001 16:02:12.2753
    Time delta from previous packet: 0.000285 seconds
    Frame Number: 2
    Packet Length: 60 bytes
    Capture Length: 60 bytes
Ethernet II
    Destination: 00:20:18:b9:49:37 (pchris.maison.mrs)
    Source: 00:20:18:61:90:e3 (gateway1.maison.mrs)
    Type: ARP (0x0806)
    Trailer: 769E858000000001000000020454E45...
Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender hardware address: 00:20:18:61:90:e3
    Sender protocol address: 192.168.0.250
    Target hardware address: 00:20:18:b9:49:37
    Target protocol address: 192.168.0.10
```

La livraison indirecte

Cette fois-ci, le transfert de données doit passer par le routeur, parce que le destinataire est dans un autre réseau logique. Prenons au hasard ftp.oleane.net:(195.25.12.28) :

```
E:\>arp -a
Aucune entrée ARP trouvée

E:\>ping 195.25.12.28

Envoi d'une requête 'ping' sur 195.25.12.28 avec 32 octets de données :

Réponse de 195.25.12.28 : octets=32 temps=30 ms TTL=245
Réponse de 195.25.12.28 : octets=32 temps=40 ms TTL=245
Réponse de 195.25.12.28 : octets=32 temps=30 ms TTL=245
Réponse de 195.25.12.28 : octets=32 temps=30 ms TTL=245

Statistiques Ping pour 195.25.12.28:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
minimum = 30ms, maximum = 40ms, moyenne = 32ms

E:\>arp -a

Interface : 192.168.0.10 on Interface 0x1000003
Adresse Internet Adresse physique Type
192.168.0.250 00-20-18-61-90-e3 dynamique
```

Que s'est-il passé ?

```
    No. Source               Destination          Protocol Info
      1 pchris.maison.mrs    ff:ff:ff:ff:ff:ff    ARP      Who has 192.168.0.250?  Tell
192.168.0.10
```

```
     2 gateway1.maison.mrs   pchris.maison.mrs     ARP      192.168.0.250 is at 00:20:18:61:90:e3
     3 pchris.maison.mrs     ftp.oleane.net        ICMP     Echo (ping) request
     4 ftp.oleane.net        pchris.maison.mrs     ICMP     Echo (ping) reply
     5 pchris.maison.mrs     ftp.oleane.net        ICMP     Echo (ping) request
     6 ftp.oleane.net        pchris.maison.mrs     ICMP     Echo (ping) reply
     7 pchris.maison.mrs     ftp.oleane.net        ICMP     Echo (ping) request
     8 ftp.oleane.net        pchris.maison.mrs     ICMP     Echo (ping) reply
     9 pchris.maison.mrs     ftp.oleane.net        ICMP     Echo (ping) request
    10 ftp.oleane.net        pchris.maison.mrs     ICMP     Echo (ping) reply
```

La requête ARP a porté sur la passerelle par défaut (gw1) parce que la couche 2 ne sait pas franchir les routeurs, elle ne sait transporter l'information que sur un seul réseau physique. Son travail se borne donc à transporter l'information jusqu'à la passerelle qui remontera la trame jusqu'au niveau 3 (IP) pour la passer ensuite sur un autre réseau.

La table ARP d'un hôte ne peut donc contenir que des adresses MAC d'hôtes ou de passerelles situées sur le même réseau physique.

Un peu plus loin, nous allons essayer de voir comment un paquet voyage en l'espionnant de chaque côté d'une passerelle.

Manipulations

Objectif de la manipulation

Nous allons essayer de décortiquer le mieux possible le fonctionnement du routage en essayant d'ouvrir un dialogue avec un hôte situé dans un autre réseau et en regardant au moyen d'un "sniffeur" ce qu'il se passe, du moins à notre portée.

Description de la manipulation

Il existe dans tous les systèmes TCP/IP une commande qui s'appelle "traceroute". Cette commande a pour but de repérer toutes les passerelles franchies pour aller de son poste à un hôte distant. En plus de déterminer les passerelles, elle indique, un peu à la manière d'un ping, le temps que met cette passerelle à répondre.

Cette commande, dans les systèmes Windows, s'appelle "tracert", sans doute à cause d'une vieille habitude de créer des noms de 8 caractères maximum. Sous Linux, elle s'appelle "traceroute". Les deux commandes donnent les mêmes indications, celle de Linux étant un peu plus puissante dans la mesure où elles est plus paramétrable.

Exemple :

Emploi de la commande "tracert" pour étudier le chemin emprunté pour aller de mon poste de travail à Marseille sur le serveur web de l'académie de Montpellier (ça change un peu d'Oléane et ce n'est pas bien loin).

```
E:\>tracert www.ac-montpellier.fr

Détermination de l'itinéraire vers mtn.ac-montpellier.fr [193.48.169.69]
avec un maximum de 30 sauts :

1 <10 ms <10 ms <10 ms gw1.maison.mrs [192.168.0.250]
2  20 ms  20 ms  30 ms ca-ol-marseille-1-2.abo.wanadoo.fr [62.161.96.2]
3  20 ms  30 ms  30 ms 194.250.158.157
4  30 ms  20 ms   *    POS-6-0-0.NCMAR202.Marseille.raei.francetelecom.net [194.51.171.41]
5  20 ms  21 ms  20 ms P0-7.ncmar302.Marseille.francetelecom.net [193.252.101.78]
6  20 ms  20 ms  30 ms P0-2.nrlyo102.Lyon.francetelecom.net [193.252.101.150]
7  30 ms  40 ms   *    P7-0.ntsta102.Paris.francetelecom.net [193.251.126.98]
8  30 ms  30 ms  41 ms 193.251.126.26
9  30 ms  31 ms  20 ms P1-0.BOUBB1.Paris.opentransit.net [193.251.128.66]
10 30 ms  40 ms  20 ms nio-i.cssi.renater.fr [193.51.206.41]
11 40 ms  40 ms  40 ms nio-n1.cssi.renater.fr [193.51.206.9]
12 70 ms  60 ms  60 ms montpellier.cssi.renater.fr [195.220.99.166]
13  *     80 ms 220 ms NRCP-montpellier.cssi.renater.fr [195.220.99.174]
14 60 ms  50 ms  60 ms 193.50.61.110
15 60 ms  60 ms  60 ms 193.48.170.21
16 60 ms  60 ms  50 ms 193.48.168.72
17 60 ms  60 ms  70 ms 193.48.169.69

Itinéraire déterminé.
```

Ce n'est pas bien loin, tout de même... 17 passerelles et il suffit de lire les noms pour constater que l'on passe par Paris! (Heureusement qu'on ne fait pas ça en voiture !).

Le réseau Renater est un réseau qui relie en France toutes les facultés et les centres de recherche.

Visiblement, le passage du réseau francetelecom au réseau renater se fait à Paris. Il n'empêche que les paquets ne mettent qu'environ 70 ms pour faire l'aller-retour.

Comment ça marche ?

La commande s'appuie sur le "Time To Live" d'un paquet de données. Ce TTL dispose d'une valeur initiale, généralement entre 15 et 30 secondes, et est décrémenté à chaque passage de routeur. La décrémentation à chaque routeur est au moins d'une seconde, plus si le paquet reste en file d'attente dans le routeur plus d'une seconde. Dans un tel cas, le TTL est décrémenté à chaque seconde passée dans la file d'attente.

Si le TTL devient nul, le paquet est considéré comme mort et est détruit par le routeur. L'émetteur du paquet reçoit un message ICMP "Time-to-live exceeded" pour le prévenir (une des raisons pour laquelle il ne faut pas filtrer tout le trafic ICMP sur un firewall).

C'est cette propriété qui va servir à définir la route. La cible envoie un premier paquet avec un TTL de 1s. Ce paquet, en arrivant sur le premier routeur, va voir son TTL tomber à 0, donc va être détruit, et le routeur va en informer l'émetteur au moyen d'un message ICMP "TTL expiré". L'opération est effectuée par défaut trois fois (les trois indices de temps indiqués dans la réponse), puis, un nouvel essai sera fait, avec cette fois-ci un TTL de 2 secondes. Normalement, le paquet doit passer le premier routeur et être détruit par le second. Ainsi de suite jusqu'à arriver à destination.

Les paquets envoyés par la source peuvent être des paquets UDP ou ICMP. La commande "traceroute" de Linux envoie par défaut des paquets UDP, mais la directive "-I" force l'émission de paquets ICMP. Sous Windows, la commande "tracert" ne sait envoyer que des paquets ICMP. Notez que l'envoi de paquets UDP peut parfois poser des problèmes.

Comment les routeurs connaissent-ils les routes ?

Là, je n'ai pas de routeur Internet sous la main pour vous montrer; cependant, le choix des routes commence déjà sur votre machine et la commande "route" permet d'administrer ces routes. C'est le même principe qui sera appliqué sur un routeur.

Voyons déjà les routes connues par mon poste de travail sous Windows 2000:

```
E:\>route print
===========================================================================
Liste d'Interfaces
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 20 18 b9 49 37 ...... Realtek RTL8029(AS) Ethernet Adapt
===========================================================================
===========================================================================
Itinéraires actifs :
Destination réseau    Masque réseau  Adr. passerelle   Adr. interface Métrique
          0.0.0.0          0.0.0.0    192.168.0.250    192.168.0.10       1    (1)
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1    (2)
      192.168.0.0    255.255.255.0     192.168.0.10    192.168.0.10       1    (3)
     192.168.0.10  255.255.255.255        127.0.0.1       127.0.0.1       1    (4)
    192.168.0.255  255.255.255.255     192.168.0.10    192.168.0.10       1    (5)
        224.0.0.0        224.0.0.0     192.168.0.10    192.168.0.10       1    (6)
  255.255.255.255  255.255.255.255     192.168.0.10    192.168.0.10       1    (7)
Passerelle par défaut :     192.168.0.250                                      (8)
===========================================================================
```

A première vue, ça semble plutôt illisible, mais avec un peu d'habitude, on y arrive assez bien:

1. Destination 0.0.0.0

C'est la route que les paquets vont prendre lorsqu'ils n'on pas trouvé un meilleur chemin. En fait, c'est la route par défaut, reprise à la ligne 8.
C'est la ligne la plus intéressante, parce qu'elle fait intervenir une adresse de passerelle (192.168.0.250 c'est à dire gw1) et une adresse d'interface (192.168.0.10) différentes.
Cette ligne veut dire en français, "Lorsqu'on ne sait pas par où il faut passer, on va emprunter l'interface 192.168.0.10 pour joindre la passerelle 192.168.0.250. C'est elle qui décidera pour la suite du chemin".

2. Destination 127.0.0.0
   C'est la boucle interne, celle qui permet à l'hôte de se parler à lui même.
3. Destination 192.168.0.0
   C'est mon réseau local. Cette ligne indique que la passerelle est 192.168.0.10, de même que l'adresse de l'interface.
4. Pour atteindre 192.168.0.10, c'est à dire moi-même, il faudra utiliser 127.0.0.1 (adresse interne toujours la même sur tous les hôtes quelque soit l'OS).
5. Pour réaliser un broadcast sur mon réseau, il faudra utiliser 192.168.0.10.
6. Si l'on souhaite faire du multicast, même chose.
7. Si l'on souhaite faire du broadcast étendu, encore la même chose.
8. La passerelle par défaut est indiquée de façon explicite.

Comme deux exemples valent mieux qu'un, nous allons maintenant voir la table de routage de gw1, plus intéressante parce que dedans, il y a deux interfaces réseau (l'une sur le réseau local, l'autre sur le réseau FTCI).

Avant d'aller plus loin, rappelons que gw1 est connecté à l'Internet par eth0 dont l'adresse est donnée par le DHCP de FTCI (213.56.56.250 actuellement), ainsi que le masque de sous réseau (255.255.248.0) et une passerelle par défaut (213.56.56.1).

```
[root@gw1 /root]# route -n
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
192.168.0.0     *               255.255.255.0   U     0      0        0 eth1 (1)
213.56.56.0     *               255.255.248.0   U     0      0        0 eth0 (2)
127.0.0.0       *               255.0.0.0       U     0      0        0 lo   (3)
default         213.56.56.1     0.0.0.0         UG    0      0        0 eth0 (4)
```

Curieusement, les informations paraissent beaucoup plus lisibles, alors que le routage devrait être plus compliqué.

1. Pour atteindre le réseau 192.168.0.0 (masque 255.255.255.0), il faut passer par l'interface eth1
2. Pour atteindre le réseau 213.56.56.0 (masque 255.255.248.0), il faut passer par eth0
3. Pour atteindre le réseau 127.0.0.0, il faut passer par l'interface locale (127.0.0.1)
4. La route par défaut, celle qu'il faut prendre lorsqu'on ne sait pas laquelle prendre, c'est de joindre la passerelle 213.56.56.1 en passant par eth0

De ceci nous pouvons déjà prévoir quelque chose: Les paquets qui partiront de mon poste de travail vers un serveur quelconque de l'Internet passeront obligatoirement par 192.168.0.10 pour rejoindre 192.168.0.250. De là, ils passeront par eth0 (213.56.56.250) pour rejoindre 213.56.56.1 et c'est ce routeur qui décidera de la suite. C'est obligatoire, ça ne peut pas être autrement, ce sont les seules routes connues dans mon rayon d'action.

Comme vous avez tous suivi attentivement, vous avez pu constater que ce que je dis ici n'est pas en

accord avec ce que dit la commande "tracert" vers www.ac-montpellier.fr[5] vue plus haut. En effet, la deuxième passerelle rencontrée n'est pas 213.56.56.1 comme on peut le prévoir, mais 62.161.96.2 qui, en plus, n'est pas située dans un réseau que gw1 sait atteindre autrement qu'en passant par 213.56.56.1. Comment se fait-il qu'il n'y ait aucune trace de la passerelle par défaut attribuée par le DHCP? Pour le savoir, demandez à FTCI; j'ignore la réponse.

(Et pourtant, ça passe ;-)

Et comment font les "vrais" routeurs ?

Ils font pareil, à part que les tables sont souvent plus longues et que leurs mises à jour se font par l'intermédiaire de protocoles de dialogue entre routeurs, pour se tenir informés des changements toujours possibles. Normalement ça marche puisqu'il est tout de même assez rare d'être confronté à de réels problèmes de routage.

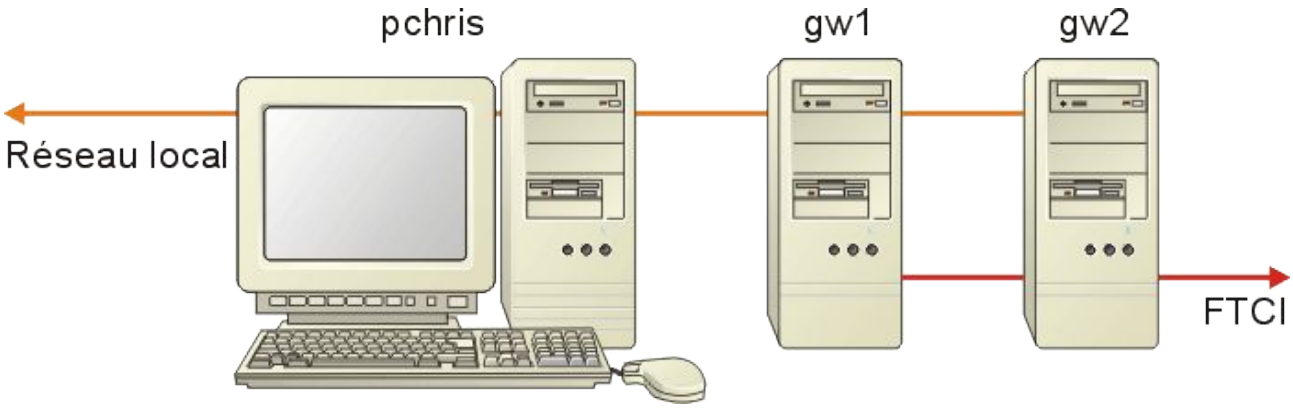
La suite

Maintenant que tout le décor est planté, passons à la manipulation proprement dite...

Pour mieux comprendre la suite de cet exposé, rappelons l'architecture sur laquelle tous les tests vont être faits :

Mon réseau local

Le réseau local est réellement constitué de 6 hôtes (gw1 et gw2 inclus). Tous les hôtes (gw1 et gw2 exclus) fonctionnent sous diverses versions de Windows. "pchris" est mon poste de travail habituel et fonctionne le plus souvent sous Windows 2000.



Connexion Internet

Il n'y a que les deux hôtes gw1 et gw2 qui sont connectés directement à l'Internet via un HUB et le Com21. Les deux machines fonctionnent sous Linux (Mandrake 7.2 à l'heure où j'écris ces lignes) et sont toutes les deux configurées en passerelles / firewall.

- gw1 est la passerelle "officielle". Normalement, il n'y a que cette machine qui est en service.
- gw2 est plus "expérimentale", cette machine n'est en service que lorsque je fais des

5 http://www.ac-montpellier.fr/

manipulations particulières, ce qui sera le cas ici.

Informations réseau

Lors des manipulations décrites dans ce chapitre, les adresses réseau étaient les suivantes:

		gw1	gw2	pchris
Eth0	**MAC**	00:20:AF:07:1A:3D	00:20:AF:4A:66:B7	00:20:18:B9:49:37
	IP	213.56.56.250	195.6.103.216	192.168.0.10
Eth1	**MAC**	00:20:18:61:90:E3	00:20:18:29:11:31	N/A
	IP	192.168.0.250	192.168.0.253	N/A
Passerelle par défaut	**MAC**	**00:00:OC:07:AC:03**	**00:00:0C:07:AC:03**	00:20:18:61:90:E3
	IP	**213.56.56.1**	**195.6.96.1**	192.168.0.250

Attention! Regardez bien les informations sur les passerelles par défaut pour gw1 et gw2 :

- Côté Internet, gw1 et gw2 ne sont pas dans les mêmes réseaux logiques.
- Leurs passerelles par défaut sont bien dans leur réseau logique.
- L'adresse MAC des deux passerelles par défaut **est la même.** Nous verrons un peu plus loin cette particularité plus en détail.

Ce qui veut dire que, bien que les deux hôtes gw1 et gw2 n'appartiennent pas au mêmes réseaux logiques (IP), ils sont malgré tout connectées sur le même réseau physique (ce qui est finalement tout à fait normal). Cette conclusion est tirée du fait que l'adresse MAC est la même pour les deux passerelles. En fait, il n'y a qu'une seule passerelle qui dispose de deux adresses IP (Plus, en réalité, comme nous le verrons plus loin).

Vérification ultime

Nous avons peut-être à voir d'un peu plus près la configuration de mon poste de travail : pchris.

La commande "ipconfig"

J'utilise Windows 2000. Ce serait la même chose avec Windows NT 4, mais pas avec WIndows 95, 98 ou Me; ces OS disposent en revanche de l'application "winipgfg" qui fait rigoureusement la même chose, mais en mode graphique.

```
E:\>ipconfig /all

Configuration IP de Windows 2000

Nom de l'hôte . . . . . . . . . . . : pchris
Suffixe DNS principal . . . . . . . : maison.mrs
Type de noeud . . . . . . . . . . . : Diffuser
Routage IP activé . . . . . . . . . : Non
Proxy WINS activé . . . . . . . . . : Non

Ethernet carte Connexion au réseau local:

Suffixe DNS spéc. à la connexion. :
Description . . . . . . . . . . . . : Carte Realtek PCI Ethernet à base RTL8029(AS)
Adresse physique. . . . . . . . . . : 00-20-18-B9-49-37
```

```
DHCP activé . . . . . . . . . . . : Non
Adresse IP. . . . . . . . . . . . : 192.168.0.10
Masque de sous-réseau . . . . . . : 255.255.255.0
Passerelle par défaut . . . . . . : 192.168.0.250
Serveurs DNS. . . . . . . . . . . : 192.168.0.250
```

C'est une configuration fixe. Il n'y a pas de DHCP sur mon réseau privé (pour 4 hôtes, ce serait peut-être excessif). Nous avons ici toutes les informations nécessaires au bon fonctionnement de la pile IP :

- Adresse MAC
- Adresse IP
- Masque de sous réseau
- Passerelle par défaut

Mais c'est quoi, cette passerelle par défaut ?

Mon poste de travail sait que tous les autres hôtes du réseau ont des adresses avec le même HostID 192.168.0.0 et qu'il peut leur envoyer directement les informations. En revanche, pour tout hôte qui dispose d'une adresse IP avec un HostID autre, il sait qu'il ne peut pas leur envoyer d'informations directement. Dans ce cas, il lui faut un relais et ce relais, c'est justement la passerelle par défaut. Ici, la configuration est simple, il n'y a qu'un seul routeur. Sur des réseaux plus complexes, il pourrait y avoir plusieurs routeurs, chacun établissant une passerelle vers des réseaux différents. La table de routage serait alors plus compliquée, une simple passerelle par défaut ne pouvant plus suffire.

Plus simplement, la couche 3 de mon OS, lorsqu'elle doit envoyer des informations à un hôte qui n'est pas sur mon réseau, se contentera de les envoyer à la passerelle par défaut, soit 192.168.0.250 qui, elle, est directement accessible, puisqu'elle est dans le même réseau logique. C'est elle qui devra se charger de définir la suite de la route.

Une route simple

Nous allons voir de très près comment déterminer l'itinéraire entre un client et le serveur FTP ftp.oleane.net. Ce n'est pas très difficile, nous savons maintenant qu'il existe une commande exprès pour.

Cette fois-ci, nous allons utiliser "tracert" sur ftp.oleane.net[6].

Quelles informations obtient-on ?

L'exemple qui suit est réalisé avec Windows 2000 depuis mon poste "pchris" :

```
Détermination de l'itinéraire vers ftp.oleane.net [195.25.12.28] avec un maximum de 30 sauts:
 1 <10 ms <10 ms <10 ms  gw1.maison.mrs [192.168.0.250]
 2  20 ms  30 ms  20 ms  ca-ol-marseille-1-2.abo.wanadoo.fr [62.161.96.2]
 3  30 ms  10 ms  30 ms  194.250.158.162
 4  30 ms  20 ms  30 ms  212.234.244.93
 5  10 ms  30 ms  20 ms  POS-6-0-0.NCMAR201.Marseille.raei.francetelecom.net [194.51.171.37]
 6  20 ms  30 ms  20 ms  P0-2.nrlyo101.Lyon.francetelecom.net [193.252.101.74]
 7  30 ms  30 ms  40 ms  P7-0.ntaub101.Aubervilliers.francetelecom.net [193.251.126.226]
 8  40 ms  30 ms  30 ms  P9-0.nraub201.Aubervilliers.francetelecom.net [193.251.126.165]
 9  30 ms   *     40 ms  POS-2-0.ARCG1.Archives.raei.francetelecom.net [194.51.159.234]
10  30 ms  40 ms  21 ms  POS-1-0.GENG1.Archives.raei.francetelecom.net [194.51.159.154]
11  40 ms  30 ms  40 ms  ftp.oleane.net [195.25.12.28]   Itinéraire déterminé.
```

6 http://ftp.oleane.net/

Comme nous l'avons vu, la commande permet d'identifier tous les routeurs par lesquels on passe pour arriver jusqu'à la cible, avec le temps nécessaire pour atteindre chacun d'eux, un peu comme le ferait un ping. Les étoiles indiquent que le temps de réponse a été trop long ou qu'il n'y a pas eu de réponse.

Comment ça marche ?

Première vérification

```
No. Source                                          Destination       Proto Info
1 - Première passerelle (la mienne). Nous voyons les trois pings et les trois réponses ICMP
On passe du réseau 192.168.0.0 au réseau 213.56.56.0 (L'adresse indiquée dans le tracert semble
ne pas être la bonne, mais souvenez-vous que ce routeur a plusieurs adresses IP
sur la même interface)
 583 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 584 gw1.maison.mrs                                 pchris.maison.mrs ICMP  Time-to-live exceeded
 585 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 586 gw1.maison.mrs                                 pchris.maison.mrs ICMP  Time-to-live exceeded
 587 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 588 gw1.maison.mrs                                 pchris.maison.mrs ICMP  Time-to-live exceeded
2 - Seconde passerelle (ma passerelle par défaut)
On passe du réseau 213.56.56.0 au réseau 194.250.158.0
 610 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 611 ca-ol-marseille-1-2.abo.wanadoo.fr             pchris.maison.mrs ICMP  Time-to-live exceeded
 612 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 613 ca-ol-marseille-1-2.abo.wanadoo.fr             pchris.maison.mrs ICMP  Time-to-live exceeded
 614 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 615 ca-ol-marseille-1-2.abo.wanadoo.fr             pchris.maison.mrs ICMP  Time-to-live exceeded
3 - Troisième passerelle
Du réseau 194.250.158.0 au réseau 194.51.171.0
 637 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 638 194.250.158.162                                pchris.maison.mrs ICMP  Time-to-live exceeded
 639 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 640 194.250.158.162                                pchris.maison.mrs ICMP  Time-to-live exceeded
 641 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 642 194.250.158.162                                pchris.maison.mrs ICMP  Time-to-live exceeded
4 - Et ainsi de suite jusqu'à la destination...
 744 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 745 212.234.244.93                                 pchris.maison.mrs ICMP  Time-to-live exceeded
 746 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 747 212.234.244.93                                 pchris.maison.mrs ICMP  Time-to-live exceeded
 748 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 749 212.234.244.93                                 pchris.maison.mrs ICMP  Time-to-live exceeded
5 -
 842 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 843 POS-6-0-0.NCMAR201.Marseille.raei.francetelecom.net pchris.maison.mrs ICMP  Time-to-live
exceeded
 844 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 845 POS-6-0-0.NCMAR201.Marseille.raei.francetelecom.net pchris.maison.mrs ICMP  Time-to-live
exceeded
 846 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 847 POS-6-0-0.NCMAR201.Marseille.raei.francetelecom.net pchris.maison.mrs ICMP  Time-to-live
exceeded
6 -
 869 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 870 P0-2.nrlyo101.Lyon.francetelecom.net           pchris.maison.mrs ICMP  Time-to-live exceeded
 871 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 872 P0-2.nrlyo101.Lyon.francetelecom.net           pchris.maison.mrs ICMP  Time-to-live exceeded
 873 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 874 P0-2.nrlyo101.Lyon.francetelecom.net           pchris.maison.mrs ICMP  Time-to-live exceeded
7 -
 896 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 897 P7-0.ntaub101.Aubervilliers.francetelecom.net  pchris.maison.mrs ICMP  Time-to-live exceeded
 898 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 899 P7-0.ntaub101.Aubervilliers.francetelecom.net  pchris.maison.mrs ICMP  Time-to-live exceeded
 900 pchris.maison.mrs                              ftp.oleane.net    ICMP  Echo (ping) request
 901 P7-0.ntaub101.Aubervilliers.francetelecom.net  pchris.maison.mrs ICMP  Time-to-live exceeded
8 -
```

```
 923 pchris.maison.mrs                                ftp.oleane.net    ICMP  Echo (ping) request
 924 P9-0.nraub201.Aubervilliers.francetelecom.net    pchris.maison.mrs ICMP  Time-to-live exceeded
 925 pchris.maison.mrs                                ftp.oleane.net    ICMP  Echo (ping) request
 926 P9-0.nraub201.Aubervilliers.francetelecom.net    pchris.maison.mrs ICMP  Time-to-live exceeded
 927 pchris.maison.mrs                                ftp.oleane.net    ICMP  Echo (ping) request
 928 P9-0.nraub201.Aubervilliers.francetelecom.net    pchris.maison.mrs ICMP  Time-to-live exceeded
9 - Notez ici la réponse qui a trop tardé à venir et considérée comme perdue
Elle se traduit dans la réponse de tracert par une astérisque
 950 pchris.maison.mrs                                ftp.oleane.net    ICMP  Echo (ping) request
 951 POS-2-0.ARCG1.Archives.raei.francetelecom.net    pchris.maison.mrs ICMP  Time-to-live exceeded
 952 pchris.maison.mrs                                ftp.oleane.net    ICMP  Echo (ping) request
1021 pchris.maison.mrs                                ftp.oleane.net    ICMP  Echo (ping) request
1022 POS-2-0.ARCG1.Archives.raei.francetelecom.net    pchris.maison.mrs ICMP  Time-to-live exceeded
10 -
1044 pchris.maison.mrs                                ftp.oleane.net    ICMP  Echo (ping) request
1045 POS-1-0.GENG1.Archives.raei.francetelecom.net    pchris.maison.mrs ICMP  Time-to-live exceeded
1046 pchris.maison.mrs                                ftp.oleane.net    ICMP  Echo (ping) request
1047 POS-1-0.GENG1.Archives.raei.francetelecom.net    pchris.maison.mrs ICMP  Time-to-live exceeded
1048 pchris.maison.mrs                                ftp.oleane.net    ICMP  Echo (ping) request
1049 POS-1-0.GENG1.Archives.raei.francetelecom.net    pchris.maison.mrs ICMP  Time-to-live exceeded
11 -
1071 pchris.maison.mrs                                ftp.oleane.net    ICMP  Echo (ping) request
1072 ftp.oleane.net                                   pchris.maison.mrs ICMP  Echo (ping) reply
1073 pchris.maison.mrs                                ftp.oleane.net    ICMP  Echo (ping) request
1074 ftp.oleane.net                                   pchris.maison.mrs ICMP  Echo (ping) reply
1075 pchris.maison.mrs                                ftp.oleane.net    ICMP  Echo (ping) request
1076 ftp.oleane.net                                   pchris.maison.mrs ICMP  Echo (ping) reply
```

Ce premier aperçu ne nous montre pas grand chose, finalement; si ce n'est que la commande "tracert" utilise des pings vers la cible et que ce sont tour à tour les passerelles successives qui répondent par un "TTL expiré", jusqu'à la cible qui répond au ping.

Essayons tout de même d'en savoir un peu plus

Nous allons regarder de plus près le contenu de la première trame émise :

```
Frame 583 (106 on wire, 106 captured)
    Arrival Time: Jan 21, 2001 10:25:11.5597
    Time delta from previous packet: 0.000000 seconds
    Frame Number: 583
    Packet Length: 106 bytes
    Capture Length: 106 bytes
Ethernet II
    Destination: 00:20:18:61:90:e3 (00:20:18:61:90:e3)
    *** Adresse MAC de l'interface Eth1 de ma passerelle linux!
    Source: 00:20:18:b9:49:37 (pchris.maison.mrs)
    *** Adresse MAC de mon poste de travail
    Type: IP (0x0800)
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 92
    Identification: 0x3b7b
    Flags: 0x00
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 1
    *** Avec un TTL de 1 seconde (comme c'est dit dans les écritures)
    Protocol: ICMP (0x01)
    Header checksum: 0xee3e (correct)
    Source: pchris.maison.mrs (192.168.0.10)
    *** Niveau IP la source est toujours mon poste de travail
    Destination: ftp.oleane.net (195.25.12.28)
    *** Niveau IP la destination est bien ftp.oleane.net
```

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xd0ff (correct)
    Identifier: 0x0200
    Sequence number: 25:00
    Data (64 bytes)
    0  0000 0000 0000 0000 0000 0000 0000 0000   ................
   10  0000 0000 0000 0000 0000 0000 0000 0000   ................
   20  0000 0000 0000 0000 0000 0000 0000 0000   ................
   30  0000 0000 0000 0000 0000 0000 0000 0000   ................
    *** Les données n'ont aucun intérêt, c'est le type ICMP qui importe
```

Nous avons constaté ici quelques détails intéressants :

- Pour le premier ping, le TTL est bien fixé à une seconde.
- Bien que la cible IP soit ftp.oleane.net, la cible Ethernet (Adresses MAC) **est la passerelle!**

Mais voyons maintenant la première réponse :

```
Frame 584 (154 on wire, 154 captured)
    Arrival Time: Jan 21, 2001 10:25:11.5599
    Time delta from previous packet: 0.000171 seconds
    Frame Number: 584
    Packet Length: 154 bytes
    Capture Length: 154 bytes
Ethernet II
    Destination: 00:20:18:b9:49:37 (pchris.maison.mrs)
    *** oui, normal...
    Source: 00:20:18:61:90:e3 (00:20:18:61:90:e3)
    *** Et c'est ma passerelle qui répond. C'est normal aussi
        C'est elle qui a tué le paquet en mettant son TTL à 0
    Type: IP (0x0800)
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
        1100 00.. = Differentiated Services Codepoint: Class Selector 6 (0x30)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 140
    Identification: 0xfb43
    Flags: 0x00
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (0x01)
    Header checksum: 0x3d18 (correct)
    Source: gw1.maison.mrs (192.168.0.250)
    Destination: pchris.maison.mrs (192.168.0.10)
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (TTL equals 0 during transit)
    *** Vous constaterez que l'on a ici toute l'explication du fonctionnement.
    Checksum: 0xf2ff (correct)
```

Avez-vous compris le principe? Nous n'allons pas toutes les faire, nous allons juste regarder un dialogue un peu plus loin pour vérifier.

La trame 923 (ne vous étonnez pas des numéros de trames, je n'étais pas le seul sur le réseau lorsque j'ai récupéré la trace, il a fallu filtrer un peu). Cette trame correspond à la première réponse du 8° routeur (P9-0.nraub201.Aubervilliers.francetelecom.net)

```
Frame 923 (106 on wire, 106 captured)
    Arrival Time: Jan 21, 2001 10:25:27.9036
    Time delta from previous packet: 0.965007 seconds
    Frame Number: 923
```

```
    Packet Length: 106 bytes
    Capture Length: 106 bytes
Ethernet II
    Destination: 00:20:18:61:90:e3 (00:20:18:61:90:e3)
    Source: 00:20:18:b9:49:37 (pchris.maison.mrs)
    *** Bien entendu, rien n'a changé, au niveau MAC, la remarque faite plus haut se re vérifie)
    Type: IP (0x0800)
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 92
    Identification: 0x3c20
    Flags: 0x00
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 8
    *** Le TTL est ici de 8 (c'est normal, on cherche la 8° passerelle)
    Protocol: ICMP (0x01)
    Header checksum: 0xe699 (correct)
    Source: pchris.maison.mrs (192.168.0.10)
    Destination: ftp.oleane.net (195.25.12.28)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xbbff (correct)
    Identifier: 0x0200
    Sequence number: 3a:00
```

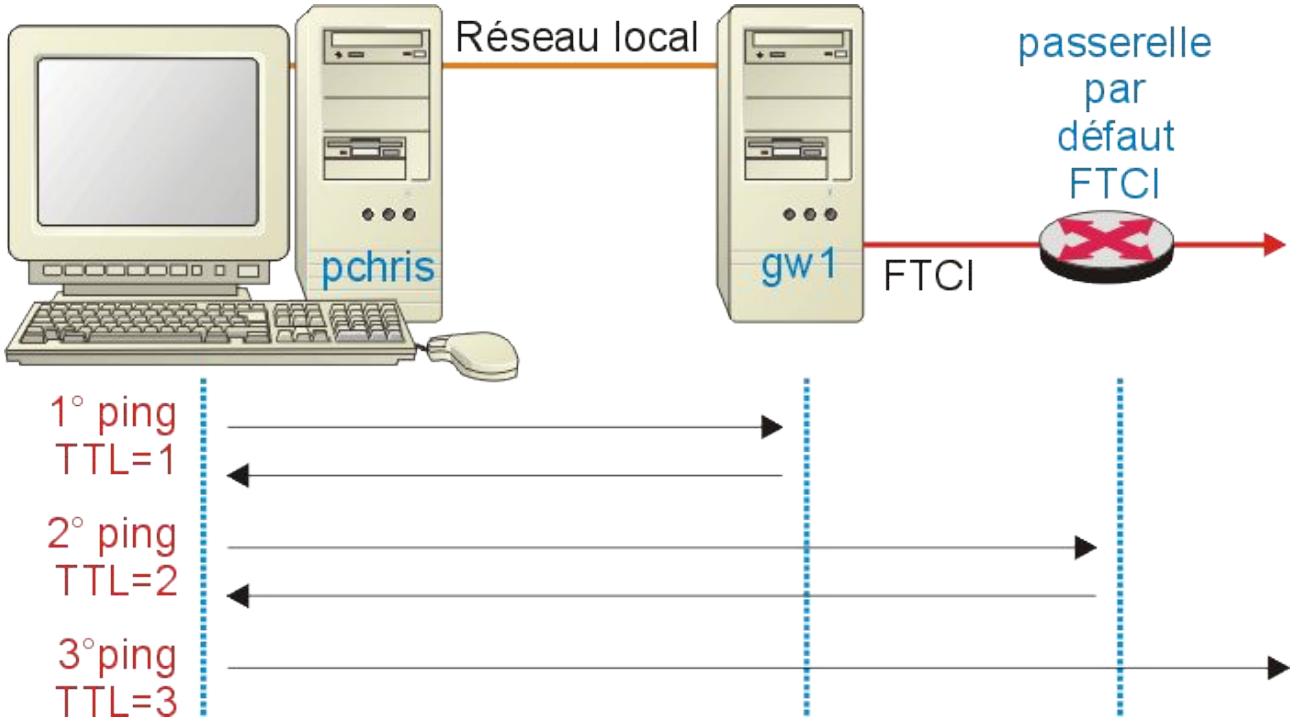
Et la réponse du 8° routeur...

```
Frame 924 (70 on wire, 70 captured)
    Arrival Time: Jan 21, 2001 10:25:27.9379
    Time delta from previous packet: 0.034276 seconds
    Frame Number: 924
    Packet Length: 70 bytes
    Capture Length: 70 bytes
Ethernet II
    Destination: 00:20:18:b9:49:37 (pchris.maison.mrs)
    Source: 00:20:18:61:90:e3 (00:20:18:61:90:e3)
    *** Et la source? C'est pas le 8° routeur, c'est toujours ma passerelle à moi!
    *** (Nous sommes au niveau 2, au niveau Ethernet)
    Type: IP (0x0800)
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 56
    Identification: 0x0000
    Flags: 0x00
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 249
    Protocol: ICMP (0x01)
    Header checksum: 0xc071 (correct)
    Source: P9-0.nraub201.Aubervilliers.francetelecom.net (193.251.126.165)
    *** Au niveau 3 (IP), c'est bien le routeur qui répond
    Destination: pchris.maison.mrs (192.168.0.10)
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (TTL equals 0 during transit)
    Checksum: 0xec57 (correct)
```

Si je n'avais pas eu peur de vous fatiguer (ce qui, du reste, est peut-être tout de même le cas), je vous aurai laissé la totalité de la trace pour vérifier que, quelque soit le routeur qui tue le ping parce que son TTL a expiré durant le transit, l'adresse MAC de la source que reçoit mon poste de travail est **toujours** celle de ma passerelle (le premier routeur que je rencontre sur le chemin). Ceci confirme bien ce que nous avons déjà vu à propos de la couche 2.

De l'autre côté...

Nous avons vu en détail le dialogue ICMP sur le réseau local. C'est bien, mais nous allons faire mieux... Un petit dessin



Grâce à gw2, nous allons espionner les paquets ICMP qui traversent gw1 pour aller plus loin. La première salve, celle qui avait un TTL de 1 en partant de mon poste de travail, nous ne la verrons pas au delà de gw1, c'est normal, gw1 l'a tuée. La première que nous verrons passer, c'est celle qui partait de pchris avec un TTL de 2.

Pour mieux suivre, nous comparons ces paquets avant passage de gw1 et après:

Envoi de l'écho.

Sur le réseau local... (entre pchris et gw1)	Sur la connexion Internet... (entre gw1 et la passerelle FTCI)

```
Frame 610 (106 on wire, 106 captured)
...
Ethernet II
    Destination: 00:20:18:61:90:e3 (eth1 sur gw1)
    Source: 00:20:18:b9:49:37 (pchris)
    *** notez bien au passage de gw1 le changement
        d'adresses MAC source et destination
...
    Time to live: 2
...
    Protocol: ICMP (0x01)
    Header checksum: 0xed31 (correct)
    Source: (192.168.0.10)
    *** Attention à l'IP...
    Destination: ftp.oleane.net (195.25.12.28)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
...
    Sequence number: 28:00
...
```

```
Frame 32 (106 on wire, 106 captured)
...
Ethernet II
    Destination: 00:00:0c:07:ac:03 (passerelle FTCI)
    Source: 00:20:af:07:1a:3d (eth0 sur gw1)
...
...
...
    Time to live: 1
    *** Le TTL a été décrémentée par gw1
    Protocol: ICMP (0x01)
    Header checksum: 0xa0b1 (correct)
    Source: (213.56.56.250)
    *** ça, c'est le travail de "IP Masquerade"
    Destination: ftp.oleane.net (195.25.12.28)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
...
    Sequence number: 28:00
...
```

Plusieurs points sont à retenir:

- Au niveau Ethernet (niveau 2) les adresses MAC ont changé, elles correspondent chaque fois à l'émetteur et au destinataire **dans** le réseau concerné.
- Le TTL du paquet a été décrémenté au passage de gw1. Nous savons déjà que, lorsque ce paquet va arriver sur la passerelle FTCI, il va être tué puisque son TTL va tomber à 0 et que cette passerelle va nous renvoyer un message ICMP "Time-to-live exceeded".
- L'adresse IP a été modifiée, mais ceci est dû au masquage d'adresse introduit par gw1. Si gw1 avait été un "vrai" routeur, il n'aurait pas agi au niveau de l'IP

Réception de la réponse

(asseyez-vous confortablement, il va y avoir des surprises)

Sur le réseau local... (entre pchris et gw1)	Sur la connexion Internet... (entre gw1 et la passerelle FTCI)
Frame 611 (70 on wire, 70 captured) ... Ethernet II Destination: 00:20:18:b9:49:37 (pchris.maison.mrs) Source: 00:20:18:61:90:e3 (eth1 sur gw1) Type: IP (0x0800) Internet Protocol ... Source: ca-ol-marseille-1-2.abo.wanadoo.fr (62.161.96.2) Destination: pchris.maison.mrs (192.168.0.10) Internet Control Message Protocol Type: 11 (Time-to-live exceeded) ...	Frame 33 (70 on wire, 70 captured) ... Ethernet II Destination: 00:20:af:07:1a:3d (ca-ol-marseille-9-250.abo.wanadoo.fr) (joli nom de gw1 sur le Net) Source: 00:03:a0:83:0c:00 (ca-ol-marseille-25-2.abo.wanadoo.fr) Type: IP (0x0800) Internet Protocol ... Source: ca-ol-marseille-1-2.abo.wanadoo.fr (62.161.96.2) Destination: ca-ol-marseille-9-250.abo.wanadoo.fr (213.56.56.250) Internet Control Message Protocol Type: 11 (Time-to-live exceeded) ...

Rappelons ici le résultat de la commande tracert:

```
Détermination de l'itinéraire vers ftp.oleane.net [195.25.12.28] avec un maximum de 30 sauts:
1 <10 ms <10 ms <10 ms  gw1.maison.mrs [192.168.0.250]
```

```
2  20 ms  30 ms  20 ms  ca-ol-marseille-1-2.abo.wanadoo.fr [62.161.96.2]
3 ....
```

Nous avions déjà rencontré ce phénomène dans la présentation de la commande "tracert", nous le retrouvons identique ici.

- Déjà, est-il normal que ce soit ca-ol-marseille-1-2.abo.wanadoo.fr (62.161.96.2) qui me réponde, alors que ma passerelle par défaut est ca-ol-marseille-9-1.abo.wanadoo.fr (213.56.56.1) ? La seconde serait logique puisqu'elle est dans le même réseau que gw1 côté public, mais ce n'est pas elle qui répond. Nous pourrions penser que c'est une astuce, il est possible en effet d'attribuer plusieurs adresses IP à la même interface réseau, mais dans ce cas, l'adresse MAC devrait correspondre...
- Encore plus curieux, au niveau Ethernet, c'est 00:03:a0:83:0c:00 qui répond (ca-ol-marseille-25-2.abo.wanadoo.fr)

Résumons-nous :

- Sur un réseau "simple", il y a une passerelle par défaut, les paquets sortant vers un autre réseau et entrant depuis un autre réseau passent par elle, une analyse de trame et une étude de la table ARP le confirment.
- Ici, tout se passe de façon plus compliquée:
  - Les paquets sortant ne peuvent passer que par la passerelle par défaut paramétrée par le serveur DHCP (ici 213.56.56.1, 00:00:0c:07:ac:03) Ce n'est pas possible autrement, ma machine connectée au COm21 n'en connaît pas d'autres.
  - Les paquets entrants, en revanche, arrivent par une autre passerelle: 00:03:a0:83:0c:00. Ce qui est encore plus curieux, c'est qu'au niveau IP elle est annoncée avec l'adresse 62.161.96.2, adresse située dans un autre réseau logique que le mien (213.56.56.0)

Éléments de réponse

Actuellement sur Marseille, nous avons plusieurs réseaux logiques et donc plusieurs passerelles par défaut. Avec un peu de patience et d'aide des collègues, il m'a été possible de définir le tableau ci-dessous (qui n'est d'ailleurs peut-être pas complet) :

Réseaux logiques FTCI sur Marseille			
Réseau	**Masque**	**Passerelle**	**Adresse MAC**
62.161.96.0	255.255.248.0	62.161.96.1	00:00:0c:07:ac:03
195.6.96.0	255.255.248.0	195.6.96.1	00:00:0c:07:ac:03
213.56.56.0	255.255.248.0	213.56.56.1	00:00:0c:07:ac:03
213.56.224.0	255.255.248.0	213.56.224.1	00:00:0c:07:ac:03

Donc, une seule passerelle physique, mais qui dispose de plusieurs adresses IP. Ça n'a rien d'anormal, mais on nous cache un peu quelque chose... A la lumière des traces déjà vues, essayons de sonder un peu les adresses suivantes :

Adresse IP	Adresse MAC
62.161.96.2	00:03:a0:83:0c:00
195.6.96.2	00:03:a0:83:0c:00
213.56.56.2	00:03:a0:83:0c:00
213.56.224.2	00:03:a0:83:0c:00

Adresse IP	Adresse MAC
62.161.96.3	00:03:a0:84:f4:00
195.6.96.3	00:03:a0:84:f4:00
213.56.56.3	00:03:a0:84:f4:00
213.56.224.3	00:03:a0:84:f4:00

Vous l'avez deviné, et ça peut se vérifier, ce sont aussi des passerelles...

Il n'y a donc rien d'étonnant à ce que les réponses puissent passer par ces passerelles, plutôt que par celle qui est donnée par le client DHCP.

Quant à comprendre le fonctionnement exact de ces passerelles...

Conclusions

Que peut-on retenir de tout ça ?

Le niveau Ethernet (niveau 2 OSI)

Ce niveau utilise les adresses MAC pour acheminer les paquets. Ici, il n'est pas possible de sortir du réseau physique.

Pour y arriver, il faut des routeurs qui travaillent au niveau supérieur. Ces routeurs prennent en charge l'acheminement des paquets inter réseaux en agissant en quelque sorte comme destinataire par procuration (ou émetteur par procuration), si bien que lorsqu'un paquet est à destination d'un autre réseau, au niveau 2, il est envoyé au routeur.

Le niveau Internet Protocol (niveau 3 OSI)

A ce niveau plus évolué, les paquets sont capables de passer d'un réseau à l'autre en empruntant des routes prédéfinies en fonction des adresses réseau (NetID). C'est à ce niveau qu'un paquet sera directement transmis au destinataire si celui-ci est situé sur le même réseau logique (livraison directe) ou transmis à une passerelle qui retransmettra plus loin (livraison indirecte). De chaque côté d'un routeur, les adresses MAC changent, de manière à ce que le niveau Ethernet puisse fonctionner correctement à l'intérieur des réseaux physiques concernés.

Épilogue

J'espère que cette contribution vous aura permis d'un peu mieux comprendre comment sur l'Internet les données circulent de part le monde avec quelques chances de ne pas se perdre.

Pour ceux qui ont à mettre en place de tels systèmes, il est fondamental de bien réfléchir à l'établissement des routes. Il n'est pas rare en effet sur des réseaux locaux constitués de plusieurs sous réseau logiques, le tout connecté à l'Internet, d'avoir l'impression que tout se passe bien, alors que des paquets devant aller d'un sous réseau à l'autre empruntent des routes aberrantes, simplement parce que le routage entre les sous réseaux a été mal fait.

Pour l'utilisateur "terminal", l'internaute "classique" la route par défaut indiquée par le DHCP du fournisseur de services suffira dans l'immense majorité des cas, surtout s'il n'a aucun réseau local, mais un minimum de connaissances sur le principe lui permettra de mieux cerner d'éventuels disfonctionnements et éventuellement d'y remédier sans penser que la réinstallation de la couche IP est le seul remède possible.

Pour les plus curieux qui se lanceront dans diverses manipulations pour observer le routage, sachez que vous risquez fort de rencontrer des situations difficilement explicables. Pour reprendre une remarque qui m'a été faite sur le forum fr.comp.reseaux.ip : "Avec IP, c'est tous les jours carnaval :-))))".

Le meilleur pour la fin

Il est de bon ton, dans une oeuvre littéraire où cinématographique, d'adopter une conclusion "ouverte", c'est-à-dire qu'elle ne conclue pas. Ça permet au lecteur ou au spectateur de se fabriquer la suite de l'histoire comme il en a envie. Ça peut aussi servir, vous l'aurez constaté maintes fois, à permettre de produire une suite, pour ceux qui manqueraient d'imagination (Alien 1, 2, 3, 4 ...).

Je vous propose ici une conclusion de ce type...

Nous avons vu des traceroutes partant de chez nous vers des hôtes distants. Nous n'avons pas, et pour cause, essayé de voir la route de l'hôte distant vers chez nous. Pourquoi faire? Tout simplement parce que rien n'oblige à ce que les routes aller et retour soient les mêmes !

Vous pouvez vous amuser avec un correspondant ou, plus simplement, avec des serveurs de traceroute. Vous en trouverez quelques uns sur cette page[7]. Prenons juste un exemple :

```
Détermination de l'itinéraire de chez moi vers www.belnet.be [193.190.198.19]

 1 gw1.maison.mrs                                        192.168.0.250
 2 ca-ol-marseille-1-2.abo.wanadoo.fr                    62.161.96.2
 3 194.250.158.162                                       194.250.158.162
 4 212.234.244.93                                        212.234.244.93
 5 POS-6-0-0.NCMAR201.Marseille.raei.francetelecom.net 194.51.171.37
 6 P0-7.ncmar301.Marseille.francetelecom.net             193.252.101.74
 7 P5-1.nrlyo101.Lyon.francetelecom.net                  193.252.101.146
 8 P7-0.ntaub101.Aubervilliers.francetelecom.net         193.251.126.226
 9 193.251.126.154                                       193.251.126.154
10 So-1-0-0.BAGBB4.Paris.opentransit.net                 193.251.240.73
11 So-5-0-0.PASBB4.Paris.opentransit.net                 193.251.240.57
12 P9-0.PASBB1.Paris.opentransit.net                     193.251.240.54
13 So-1-0-3.TELBB1.Telehouse.opentransit.net             193.251.240.150
14 paris1.fr.eqip.net                                    195.206.65.141
15 paris5.fr.eqip.net                                    195.206.64.61
16 amsterdam11.nl.eqip.net                               195.90.64.217
17 amsterdam51.nl.eqip.net                               195.90.65.121
18 amsterdam9.nl.eqip.net                                195.90.65.102
19 nl-aucs.nl.ten-155.net                                212.1.194.1
20 ge.nl40.ten-155.net                                   212.1.193.146
21 nl-uk-2.uk40.ten-155.net                              212.1.197.62
22 be-uk.be1.ten-155.net                                 212.1.197.14
23 pvc0-1005.c12008.brussels.belnet.net                  212.1.192.122
24 g10-0-0.c7513.science.belnet.net                      193.190.197.182
25 dalet.belnet.be                                       193.190.198.19

Itinéraire déterminé.
```

```
Détermination de l'itinéraire de www.belnet.be [193.190.198.19] vers chez moi [213.56.56.250] :

1 g0-1-0-1.c7513.science.belnet.net                    193.190.198.16
 2 g6-0.c12008.brussels.belnet.net                      193.190.197.181
 3 serial5-0.bru-icr-02.carrier1.net                    212.4.203.1
 4 fastethernet6-1.bru-bbr-01.carrier1.net              212.4.199.197
 5 pos13-1.lon-bbr-02.carrier1.net                      212.4.199.61
 6 pos1-0.lon-bbr-01.carrier1.net                       212.4.193.189
 7 pos13-0.par-bbr-02.carrier1.net                      212.4.211.134
 8 serial1-1.par-ixr-01.carrier1.net                    212.4.192.234
 9 Oleane.parix.net                                     198.32.246.20
10 Raspail.GW.OLEANE.NET                                194.2.3.10
11 POS-8-0.NRSTA102.Raspail.raei.francetelecom.net      194.51.159.53
12 P3-0.ntsta102.Paris.francetelecom.net                193.251.126.42
13 P9-0.nrlyo102.Lyon.francetelecom.net                 193.251.126.97
14 P0-0.ncmar302.Marseille.francetelecom.net            193.252.101.149
15 P0-0-0.ncmar202.Marseille.francetelecom.net          193.252.101.77
```

7 http://www.traceroute.org/

```
16 POS-5-1-0.MAR4.Marseille.raei.francetelecom.net     194.51.171.42
17 194.250.158.158                                     194.250.158.158
18 ca-ol-marseille-9-250.abo.wanadoo.fr                213.56.56.250

Itinéraire déterminé.
```

Ce n'est pas très facile à interpréter, parce que, même lorsqu'on passe le même routeur dans un sens ou dans l'autre, on ne le voit pas avec la même adresse ni le même nom, puisqu'on le voit par l'interface par laquelle on entre. Il est clair cependant dans cet exemple que les chemins ne sont pas les mêmes à l'aller et au retour, puisqu'il n'y a pas le même nombre de passerelles franchies.

Alors, réfléchissez à ceci: vous faites un traceroute. Les messages ICMP "TTL Exceed" qui vous reviennent ne prennent pas forcément le même chemin que le ping que vous avez envoyé. La durée indiquée sur la ligne correspond aux temps aller + retour. Comme les chemins peuvent être différents, que pouvez-vous conclure ? Rien, parce qu'un temps élevé ne met pas forcément en cause la passerelle qui a répondu, mais peut être une passerelle dont on ignore tout et qui est située quelque part sur le chemin de retour, mais pas sur le chemin de l'aller.

Vertigineux non ?